This listing of claims will replace all prior versions and listings of claims in this application:

b.) Listing of Claims

1. (currently amended) A network comprising:
   a first network domain including a first routing device for routing network traffic out of and into the first network domain; and
   a monitor/regulator, either integrally disposed in said first routing device or coupled to the first routing device to monitor the network traffic routed by said first routing device, ~~and~~ that determines ~~determine~~ if the first network domain is sourcing undesirable network traffic, comprising a denial of service attack, out of the first network domain.

2. (Original) The network of claim 1, wherein said monitor/regulator makes said determination based on differential characteristics of network traffic routed out of said network domain, and network traffic routed into the network domain.

3. (Original) The network of claim 2, wherein said monitor/regulator infers said differential characteristics based on aggregated statistics of said network traffic routed out of said network domain, and aggregated statistics of said network traffic routed into the network domain.

4. (Original) The network of claim 2, wherein said monitor/regulator aggregates said differential characteristics based on differential characteristics between request packets routed out of said network domain, and response packets routed into the network domain.

5. (Original) The network of claim 1, wherein said monitor/regulator, upon determining undesirable network traffics are being sourced our of said first domain, further stops said undesirable network traffic from being sourced out of said first domain.

6. (Original) The network of claim 1, wherein

said first network domain further comprises a second routing device for routing network traffic out of and into the first network domain;

said monitor/regulator further monitors the network traffic routed by said second routing device, and determines if the first network domain is sourcing undesirable network traffic out of the first network domain based on network traffic characteristics observed of network traffic routed through said first and second routing devices.

7. (Original) The network of claim 6, wherein said monitor/regulator determines if undesirable network traffics are being routed out of said first network domain through said first routing device based on network traffic characteristics observed of network traffic routed through said second as well as said first routing device.

8. (Original) The network of claim 6, wherein said monitor/regulator determines if undesirable network traffics are being routed out of said first network domain through said second routing device based on network traffic characteristics observed of network traffic routed through said first as well as said second routing device.

9. (Original) The network of claim 6, wherein said monitor/regulator, upon determining undesirable network traffics are being sourced out of said first network domain, further stops said undesirable network traffic from being sourced out of said first network domain.

10. (Original) The network of claim 1, wherein

said network further comprises a second network domain including a second routing device for routing network traffic out of and into the second network domain;

said monitor/regulator further monitors the network traffic routed by said second routing device, and determines if at least a selected one of the first and second network domains is sourcing undesirable network traffic out of

the selected one of the first and second network domains based on network traffic characteristics observed of network traffic routed through said first and second routing devices.

11. (Original) The network of claim 10, wherein said monitor/regulator determines if undesirable network traffics are being routed out of said first network domain through said first routing device based on network traffic characteristics observed of network traffic routed through said second as well as said first routing device.

12. (Original) The network of claim 10, wherein said monitor/regulator determines if undesirable network traffics are being routed out of said second network domain through said second routing device based on network traffic characteristics observed of network traffic routed through said first as well as said second routing device.

13. (Original) The network of claim 10, wherein said monitor/regulator, upon determining undesirable network traffics are being sourced out of at least a selected one of said first and second network domains, further stops said undesirable network traffic from being sourced out of said first and second network domains.

14. (currently amended) A network traffic regulation method comprising:
monitoring network traffic routed by a first routing device of a first network domain; and
determining if the first network domain is sourcing undesirable network traffic, comprising a denial of service attack, out of the first network domain.

15. (Original) The method of claim 14, wherein said determining comprises determining based on differential characteristics of network traffic routed out of said network domain, and network traffic routed into the network domain.

16. (Original) The method of claim 15, wherein said determining comprises inferring said differential characteristics based on aggregated statistics of said network traffic routed out of said network domain, and aggregated statistics of said network traffic routed into the network domain.

17. (Original) The method of claim 15, wherein said determining comprises aggregating said differential characteristics based on differential characteristics between request packets routed out of said network domain, and response packets routed into the network domain.

18. (Original) The method of claim 14, wherein the method further comprises stopping undesirable network traffics from being sourced out of said first network domain.

19. (Original) The method of claim 14, wherein the method further comprises

monitoring network traffic routed by a second routing device of said first network domain; and

determining if the first network domain is sourcing undesirable network traffic out of the first network domain based on network traffic characteristics observed of network traffic routed through said first and second routing devices.

20. (Original) The method of claim 19, wherein said determining comprises determining if undesirable network traffics are being routed out of said first network domain through said first routing device based on network traffic characteristics observed of network traffic routed through said second as well as said first routing device.

21. (Original) The method of claim 19, wherein said determining comprises determining if undesirable network traffics are being routed out of said first network domain through said second routing device based on network traffic

characteristics observed of network traffic routed through said first as well as said second routing device.

22. (Original) The method of claim 19, wherein the method further comprises stopping undesirable network traffic from being sourced out of the first network domain.

23. (Original) The method of claim 19, wherein the method further comprises determining if at least a selected one of the first and a second network domain is sourcing undesirable network traffic out of the selected one of the first and second network domains based on network traffic characteristics observed of network traffic routed through said first and second routing devices.

24. (Original) The method of claim 23, wherein said determining comprises determining if undesirable network traffics are being routed out of said first network domain through said first routing device based on network traffic characteristics observed of network traffic routed through said second as well as said first routing device.

25. (Original) The method of claim 23, wherein said determining comprises determining if undesirable network traffics are being routed out of said second network domain through said second routing device based on network traffic characteristics observed of network traffic routed through said first as well as said second routing device.

26. (Original) The method of claim 23, wherein the method further comprises stopping undesirable network traffic from being sourced out said first and/or second network domains.

27. (currently amended) An apparatus comprising:

(a) storage medium having stored therein a plurality of programming instructions designed to enable the apparatus to monitor network traffic

routed by a first routing device of a first network domain, and determine if the first network domain is sourcing undesirable network traffic, comprising a denial of service attack, out of the first network domain; and

(b) a processor coupled the storage medium to execute the programming instructions.

28. (Original) The apparatus of claim 27, wherein the programming instructions enable the apparatus to make said determination based on differential characteristics of network traffic routed out of said network domain, and network traffic routed into the network domain.

29. (Original) The apparatus of claim 28, wherein the programming instructions enable the apparatus to infer said differential characteristics based on aggregated statistics of said network traffic routed out of said network domain, and aggregated statistics of said network traffic routed into the network domain.

30. (Original) The apparatus of claim 28, wherein the programming instructions enable the apparatus to aggregate said differential characteristics based on differential characteristics between request packets routed out of said network domain, and response packets routed into the network domain.

31. (Original) The apparatus of claim 27, wherein the programming instructions further enable the apparatus to stop undesirable network traffic from being sourced out of said first network domain.

32. (Original) The apparatus of claim 27, wherein the programming instructions enable the apparatus to monitor network traffic routed by a second routing device of said first network domain, and determine if the first network domain is sourcing undesirable network traffic out of the first network domain based on network traffic characteristics observed of network traffic routed through said first and second routing devices.

33. (Original) The apparatus of claim 32, wherein the programming instructions enable the apparatus to determine if undesirable network traffics are being routed out of said first network domain through said first routing device based on network traffic characteristics observed of network traffic routed through said second as well as said first routing device.

34. (Original) The apparatus of claim 32, wherein the programming instructions enable the apparatus to determine if undesirable network traffics are being routed out of said first network domain through said second routing device based on network traffic characteristics observed of network traffic routed through said first as well as said second routing device.

35. (Original) The apparatus of claim 32, wherein the programming instructions further enable the apparatus to stop undesirable network traffic from being sourced out said first network domain.

36. (Original) The apparatus of claim 27, wherein the programming instructions further enable the apparatus to determine if at least a selected one of the first and a second network domain is sourcing undesirable network traffic out of the selected one of the first and second network domains based on network traffic characteristics observed of network traffic routed through said first and second routing devices.

37. (Original) The apparatus of claim 36, wherein the programming instructions enable the apparatus to determine if undesirable network traffics are being routed out of said first network domain through said first routing device based on network traffic characteristics observed of network traffic routed through said second as well as said first routing device.

38. (Original) The apparatus of claim 36, wherein the programming instructions enable the apparatus to determine if undesirable network traffics are being routed out of said second network domain through said second routing device based on

network traffic characteristics observed of network traffic routed through said first as well as said second routing device.

39. (Original) The apparatus of claim 36, wherein the programming instructions further enable the apparatus to stop undesirable network traffic from being sourced out said first and/or second network domains.

40. (New) The network of claim 1, wherein said monitor/regulator monitors flows and determines whether the first network domain is sourcing undesirable network traffic based on said flows.

41. (New) The network of claim 40, wherein said monitor/regulator monitors said flows including tracking source and destination addresses and port information.

42. (New) The network of claim 1, wherein said monitor/regulator generates statistics concerning destination addresses and determines whether the first network domain is sourcing undesirable network traffic based on said statistics.

43. (New) The network of claim 1, wherein said monitor/regulator generates statistics concerning lengths of packets and determines whether the first network domain is sourcing undesirable network traffic based on said statistics.

44. (New) The network of claim 1, wherein said monitor/regulator generates statistics concerning distributions of time to live values and determines whether the first network domain is sourcing undesirable network traffic based on said statistics.

45. (New) The network of claim 1, wherein said monitor/regulator tracks differences between outbound TCP SYN and FIN packets and inbound response packets and determines whether the first network domain is sourcing undesirable network traffic based on said differences

46. (New) The network of claim 1, wherein said monitor/regulator instructs a routing device to lower a priority of the undesirable network traffic.

47. (New) The network of claim 1, wherein said monitor/regulator instructs a routing device to slow the undesirable network traffic.

48. (New) The network of claim 10, wherein said monitor/regulator, upon determining undesirable network traffics are being sourced out of at least a selected one of said first and second network domains, lower a threshold for concluding that undesirable network traffic are being sourced out of an other one of said first and second network domains.

49. (New) The method of claim 14, further comprising monitoring flows and determining whether the first network domain is sourcing undesirable network traffic based on said flows.

50. (New) The method of claim 49, wherein monitoring said flows includes tracking source and destination addresses and port information.

51. (New) The method of claim 14, further comprising generating statistics concerning destination addresses and determining whether the first network domain is sourcing undesirable network traffic based on said statistics.

52. (New) The method of claim 14, further comprising generating statistics concerning lengths of packets and determining whether the first network domain is sourcing undesirable network traffic based on said statistics.

53. (New) The method of claim 14, further comprising generating statistics concerning distributions of time to live values and determinings whether the first network domain is sourcing undesirable network traffic based on said statistics.

54. (New) The method of claim 14, further comprising tracking differences between outbound TCP SYN and FIN packets and inbound response packets and

determining whether the first network domain is sourcing undesirable network traffic based on said differences

55. (New) The method of claim 14, further comprising instructing a routing device to lower a priority of the undesirable network traffic.

56. (New) The method of claim 14, further comprising instructing a routing device to slow the undesirable network traffic.

57. (New) The method of claim 23, further comprising, upon determining undesirable network traffics are being sourced out of at least a selected one of said first and second network domains, lowering a threshold for concluding that undesirable network traffic are being sourced out of an other one of said first and second network domains.